

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;)	
)	
Petition for Rulemaking to Enhance Security And Authentication Standards for Access to Customer Proprietary Network Information)	RM-112777
)	

COMMENTS OF INSITE WIRELESS LLC

InSite Wireless LLC ("InSite") hereby submits the following reply comments, pursuant to §1.419 of the Commission's Rules, regarding the above-mentioned proceeding and in support of the comments filed by NextG Networks, Inc. ("NextG") and Crown Castle International Corp. ("Crown Castle").

I. Introduction and Summary

InSite is an infrastructure provider. As such, InSite specializes in the design, installation, management and maintenance of systems that enhance in-building wireless voice and data communications in private and public facilities. InSite is a "backend" service providing the installation of a Distributed Antenna System (DAS), a path of wireless signals distributed throughout any indoor or underground structure to aid in obtaining seamless connectivity while traveling from the macro (outdoor) environment to in-building locations for wireless device

users. InSite provides its infrastructure building services to private facility owners¹, which are then leased to large cellular carriers, PCS phone carriers, Enhanced Specialized Mobile Radio (“ESMR”), paging, and public safety two-way radios.

The current CPNI rules² and the solutions and revisions provided by the Electronic Privacy Information Center (“EPIC”) are too broad and over inclusive in application to infrastructure providers like InSite. Similar to NextG and Crown Castle, InSite does not maintain nor does it have access to end user CPNI. InSite is concerned that the current and proposed revisions to the CPNI rules, if applied to the infrastructure provider, will unduly burden the provider, both administratively and financially, offering no further protection to the retail end user. The Commission should recognize the public policy concern addressed by these rules and the proposed revisions is not served by requiring infrastructure providers like InSite to comply, and may hinder the provider’s ability to offer its services affordably and competitively. While InSite supports the positions of both NextG and Crown Castle in seeking an exemption from the rules, InSite suggests that it is even further removed from the purview of the Commission’s current and contemplated revisions of the CPNI rules, as it is merely an infrastructure provider of DAS Systems to facility owners, and cannot even be considered a “carrier’s carrier.”³ Should the Commission find that the current rules do not apply to “carrier’s carriers” like NextG and Crown Castle, it should necessarily find that they do not apply to infrastructure providers like InSite. Moreover, should the Commission decline to make this distinction, InSite respectfully requests that in considering the EPIC petition, the Commission take notice of the role of infrastructure

¹ Some of InSite’s most notable venues include The Moscone Center in San Francisco, CA, The Wynn Resort & Casino in Las Vegas, the Wisconsin Center, the Boston Convention Center, Dane County Regional Airport, Minneapolis Convention Center, MBTA, and Summerfest Wisconsin.

² Section 222 and the CPNI rules at 64.2001 *et seq.*

³ Comments of NextG at 2.

providers and make an exemption to any revisions adopted for infrastructure providers engaged only in design, installation, management and maintenance of DAS systems, and which have no access to CPNI.

II. Discussion

1. The current CPNI rules and proposed revisions should not apply to infrastructure providers like InSite, because InSite does not have access to CPNI of individual retail end users.

The Commission's current orders and CPNI rules⁴ concern and address customer proprietary information of the *individual*⁵ retail end user.⁶ Like NextG and Crown Castle, InSite does not maintain or have access to CPNI records of individual retail end users of carrier systems. As mentioned earlier, InSite primarily does business with private facility owners, who then lease these infrastructure systems to large cellular carriers. This puts InSite, at least, two-steps removed from the process of collecting, maintaining, or even coming in contact with the CPNI of individual retail end users. The information that InSite maintains is the basic information of the facility owner or large corporation, and is used primarily for billing and routine business. Any information that InSite maintains on its customer is either publicly available or protected by the contracts executed between the customer and InSite.

⁴ 47 C.F.R. § 64.2001 *et seq.*

⁵ small business and/or residential

⁶ The Commission's NPRM states that "Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. CPNI therefore includes highly-sensitive personal information." NPRM at ¶ 3.

2. The additional requirements sought by EPIC should not be required of infrastructure providers like InSite, because they would impose too great of an administrative and financial burden with no benefit to the end user.

EPIC has asked the Commission to require security measures to protect CPNI including Consumer-set passwords, Audit Trails, Encryption, and Record Destruction to avoid a security breach.⁷ As NextG points out, implementing encryption, audit trails, and passwords is costly with no added benefit to the customer.⁸ Encryption alone would require computer system upgrades to the InSite systems, which are likely to require expensive labor and service costs. Like NextG, InSite maintains a limited number of large accounts, with which InSite maintains strong business relationships. Consumer-set passwords and audit trails are simply unnecessary. It is unlikely that InSite would inadvertently release the proprietary information of these clients as the parties on both ends are very well acquainted, and as doing so would create a negative impact on that business relationship and the ability to gain new business. Likewise, destroying customer records would be extremely harmful and serve no purpose for either party involved. It is important that InSite be able to maintain its business and customer files for as long as necessary and prudent for any of a number of both offensive and defensive business reasons. Finally, InSite prides itself on being able to maintain its services at an affordable cost to its clients. If these requirements were imposed, InSite would not be able to maintain its current profit margins, and might be forced to pass on some of the cost to the customer. Although InSite's infrastructure services are unique, implementing these additional measures would be detrimental to InSite's ability to compete effectively as competition is strong for new and existing business.⁹

⁷ EPIC Petition at 11, 12.

⁸ NextG Comments, April 28, 2006, at 6-7.

⁹ Crown Castle at 4, fn. 4.

3. The underlying Public Policy reasons of § 222 are not served by applying the current CPNI rules and proposed revisions to infrastructure providers like InSite, because InSite is not a carrier under The Act.

The Commission's CPNI rules, Section 222 of the Communications Act, and the most recent NPRM concern unauthorized access to individual end user CPNI collected in large customer databases, primarily by telephone or cellular telephone carriers, which can be accessed by pretexters or hackers.¹⁰ The rules do not concern protection of infrastructure building and maintenance services, and therefore, should not implicate infrastructure providers like InSite. As discussed above, InSite does not maintain the type of CPNI needing protection, nor does it maintain such large databases of customer and client information where this CPNI is generally found and where it is most susceptible to fraudulent activity. Moreover, InSite is not as easily susceptible to pretexters or hackers because of the nature and sophistication of their business contacts. Most notably, the underlying public policy of Section 222 does not apply to InSite, because InSite is not a telecommunications carrier under The Act¹¹. Section 222 established a "duty of every telecommunications carrier to protect the confidentiality of its customers' CPNI."¹² Unlike Crown Castle¹³ and NextG¹⁴, InSite is not a carrier of any kind and does not maintain any licenses to act as a telecommunications carrier in any state.

¹⁰ NPRM at ¶¶ 9-11.

¹¹ Communications Act of 1934, as amended by the Telecommunications Act of 1996.

¹² 47 U.S.C. § 222

¹³ See Crown Castle at fn. 1.

¹⁴ NextG at 4-5.

However, as Crown Castle points out¹⁵, to the extent that InSite maintains proprietary information on any customer (i.e., technical configuration, type, destination, location, amount of use of telecommunications service subscribed to..."¹⁶), it is already in compliance with the Commission's CPNI rules as this information is either explicitly protected by contract or available to the public. Additionally, InSite does not use its customer information for marketing purposes, and customer information is never sold or otherwise accessed by third parties without the knowledge of the client.¹⁷

III. Conclusion

InSite asks the Commission to clarify the current CPNI rules as they apply to infrastructure providers like InSite. InSite respectfully submits that an exemption should be carved out for infrastructure providers as infrastructure providers have no access to retail end user CPNI and are not telecommunications carriers under the Act. Should the Commission refuse to adopt this distinction, and apply the current CPNI rules to infrastructure providers, InSite respectfully submits that the Commission find that any adoption of the EPIC proposed rules do not apply to infrastructure providers, and carve out an exemption for infrastructure providers engaged only in design, installation, management and maintenance of DAS systems. The current rules provide adequate recourse for the unauthorized access to CPNI, and further requirements are not necessary and should not be imposed on infrastructure providers as they have no access to retail end user CPNI, implementation of additional requirements would impose too great a burden on

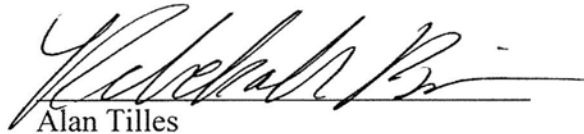
¹⁵ Crown Castle at 5.

¹⁶ 47 U.S.C. § 222(h)(1)(A)

¹⁷ See Comments of Crown Castle, April 13, 2006 at 3. 47 C.F.R. §64.20005. 47 C.F.R. § 64.20007.

the infrastructure provider with no benefit to the end user, and the underlying public policy is not served.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Alan Tilles', with a horizontal line drawn underneath it.

Alan Tilles
Rebekah Bina
Shulman, Rogers, Gandal, Pordy & Ecker
11921 Rockville Pike, 3rd Floor
Rockville, Maryland 20852
(301) 230-5200
(301)230-2891
atilles@srgpe.com
rbina@srgpe.com

David Weisman
InSite Wireless LLC
301 North Fairfax Street, Suite 101
Alexandria, VA 22314
(703) 535-3009
(703) 535-3051
dweisman@mountainuniontelecom.com

May 15, 2006